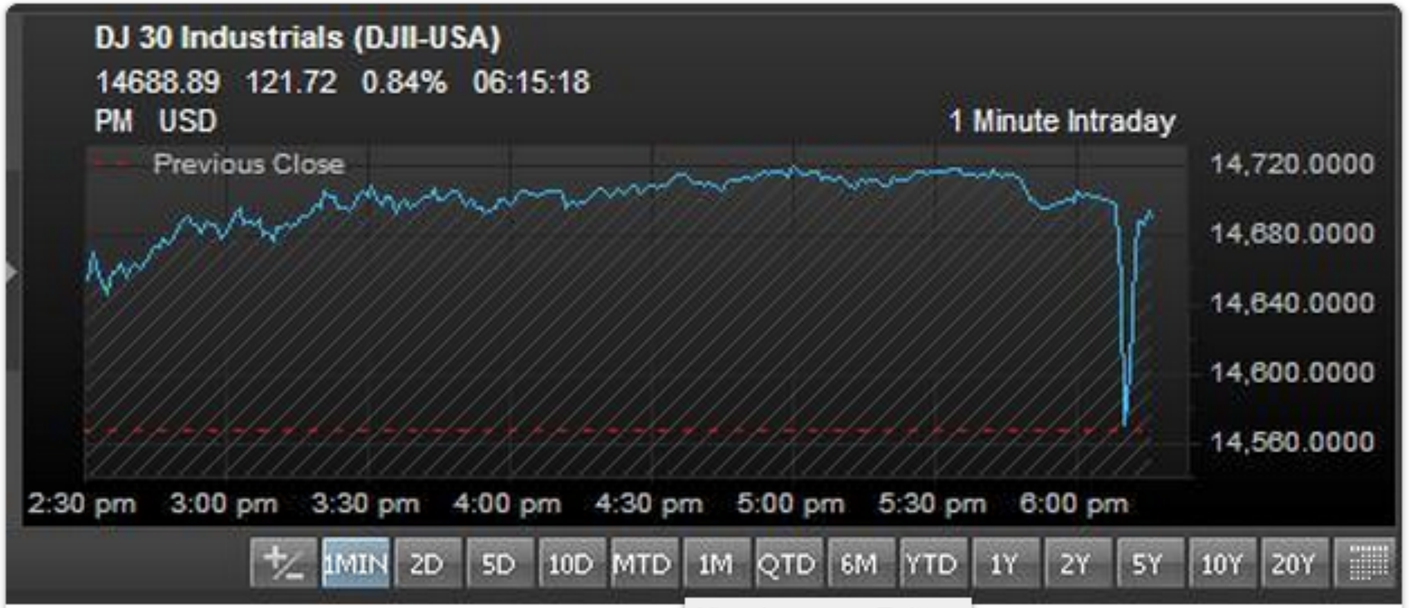
Digital Security

J215: Introduction to Multimedia

WHY DOES THIS MATTER?


AP
@AP
The Associated Press
Follow @AP
Breaking: Two Explosions in the White House and Barack Obama is injured
April 23, 2013 5:07 pm via web
Reply
Retweet
Favorite



View image on Twitter

Judd Legum
@JuddLegum

Follow

Stock market reacts to fake AP tweet
pic.twitter.com/3q1XWYPNg3 via @charlesforelle

10:19 AM - 23 Apr 2013

30 RETWEETS **3** FAVORITES

Analysis & Opinion | Jack Shafer

What was James Rosen thinking?

By Jack Shafer | May 20, 2013

232 234

Tags: FOX NEWS | JAMES ROSEN | OBAMA ADMINISTRATION | SPYING

U.S. President Barack Ob
binoculars to see North K
the DMZ, north of Seoul

Just open your Twitter feed and listen to the Washington press corps howl about the Obama administration's latest intrusion into their business.

protests of the
Channel's Brit
Keith Olbermann. All deplore, in vo
leak investigation that has criminali

While I join this chorus of rage, I al
making. Did Rosen get caught and
journalistic tradecraft?

State Dept. contractor charged in leak to news organization

By Spencer S. Hsu
Washington Post Staff Writers
Saturday, August 28, 2010

A State Department contractor was indicted Friday by a federal grand jury in the District, becoming the latest target of a series of investigations into unauthorized government leaks to news organizations under the Obama administration.

Network News PROFILE

View More Activity

TOOLBOX

Resize Print
E-mail Reprints

Stephen Jin-Woo Kim, 43, then a senior adviser for intelligence on detail to the State Department's arms control compliance bureau, was charged with disclosing national defense information in June 2009 to a national news organization, believed to be Fox News, and lying to the FBI. Kim pleaded not guilty before U.S. District Judge Colleen Kollar-Kotelly.

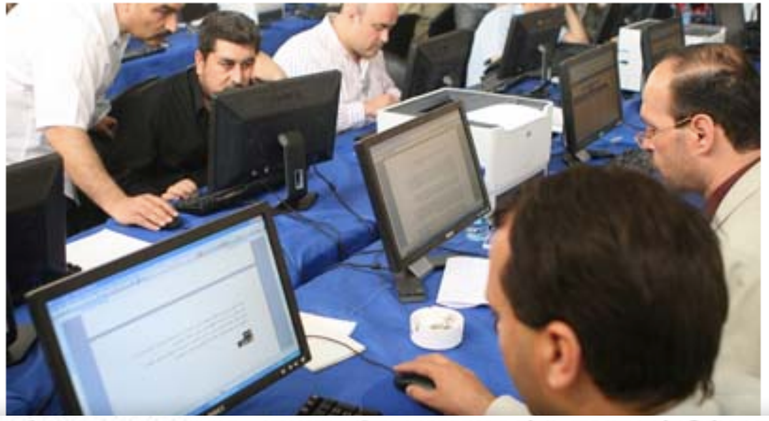
Although unnamed by the government, Fox News reporter James Rosen wrote a report posted June 11, 2009, saying that U.S. intelligence officials had warned that North Korea

Don't get your sources in Syria killed

AA Text Size Print

By Eva Galperin/CPJ Guest Blogger

Share



Becaus
uprisi
citizen
countr
threat

In late 2011, British journalist and filmmaker Sean McAllister was captured in Syria after interviewing many dissidents on film. His laptop, phone, and documents seized, McAllister had no way to protect the sources he hoped to keep safe, and many of those who claim they were in touch with McAllister have fled the country for fear of retaliation.[13]

Journalists who hope to encrypt their e-mails as a means of protecting themselves and their sources can evaluate a few basic options that require only slight technical expertise, according to Jeremy Barr at the Poynter

WIRED How Trusting in Vice Led to John McAfee's Downfall

MAT HONAN GEAR 12.06.12 6:37 PM

HOW TRUSTING IN VICE LED TO JOHN MCAFEE'S DOWNFALL

By now, YOU ARE AWARE of John McAfee . If there's one thing that the sexagenarian millionaire antivirus

concerning the murder.[77][78][79]

The magazine *Vice* accidentally gave away McAfee's location at a Guatemalan resort in early December 2012, when a photo taken by one of its journalists accompanying McAfee was posted with the EXIF geolocation metadata still attached.[80] While in Guatemala, McAfee asked Chad Essley, an American cartoonist and animator, to set up a blog so that McAfee could write about his experience while on the run.[81] McAfee then appeared publicly in Guatemala City, where he attempted to seek political asylum.

On December 5, 2012, McAfee was arrested for illegally entering Guatemala. Shortly afterward, he was placed under

DOJ's secret subpoena of AP phone records broader than initially revealed

Monday May 20, 2013 10:06 AM

The Intercept_

TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION

Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim

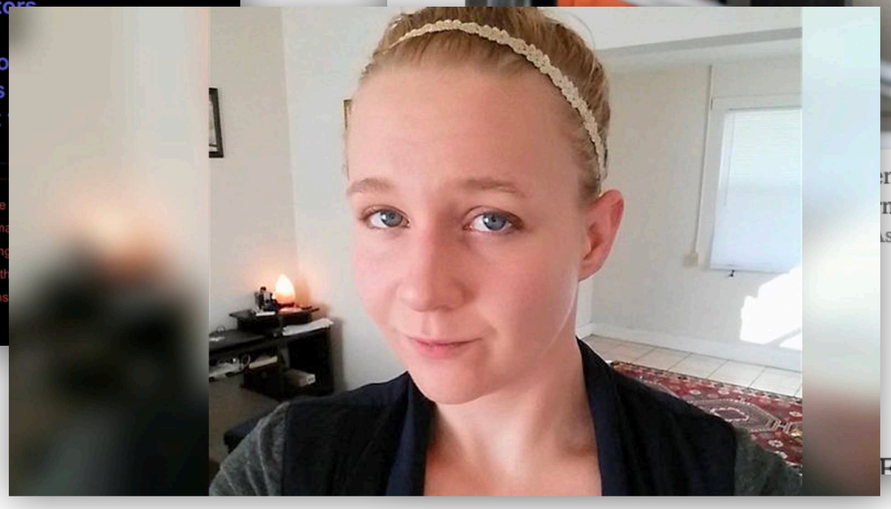
June 5 2017, 12:44 p.m.

1786

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors [redacted] Target U.S. Companies and Local U.S. Government Officials Using Vo Registration-Themed Emails, Spoof Election-Related Products Services, Research Absentee Ballot Email Addresses; August November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

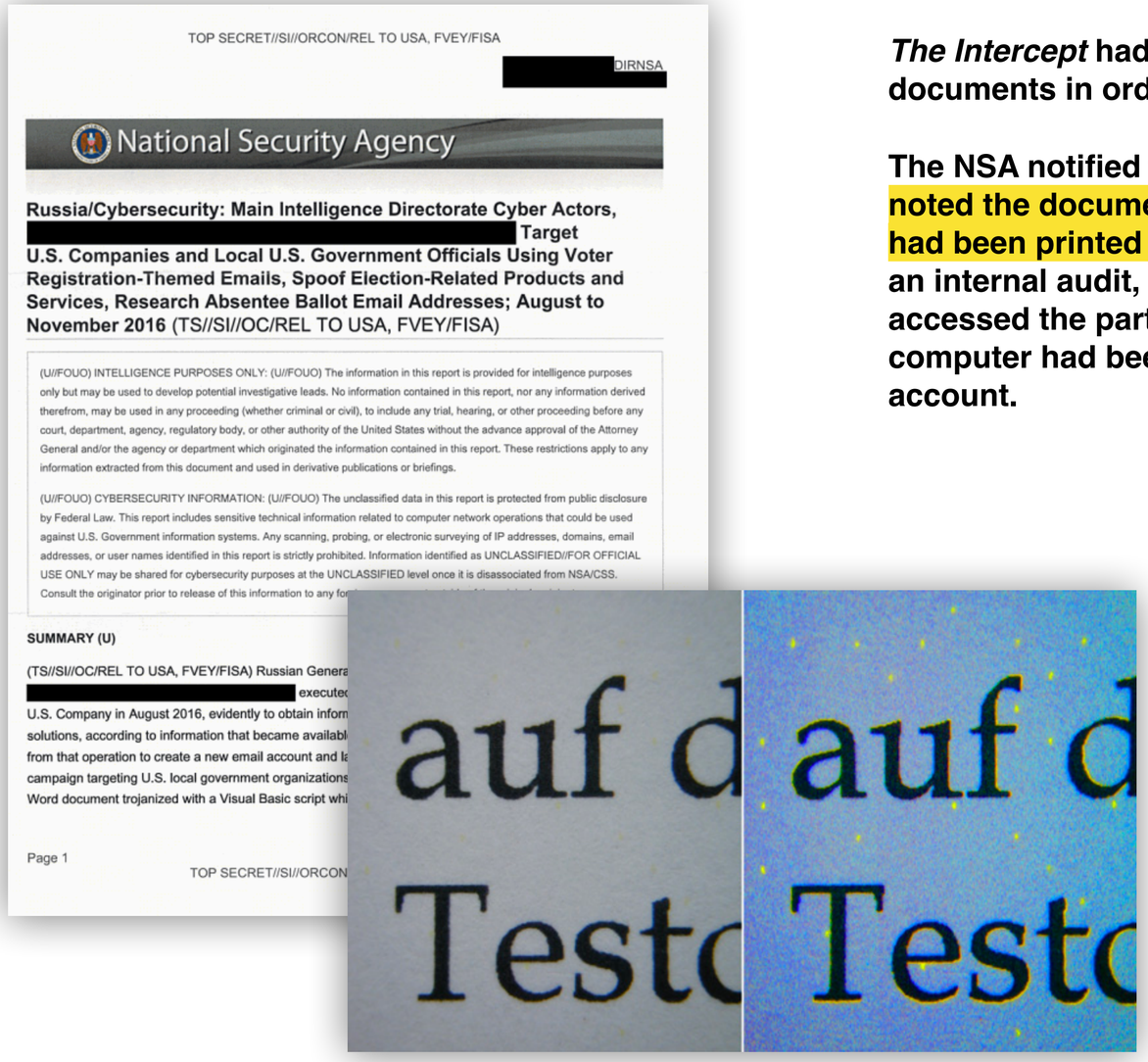
(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence only but may be used to develop potential investigative leads. No information contained in this report, nor any informa therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding court, department, agency, regulatory body, or other authority of the United States without the advance approval of t General and/or the agency or department which originated the information contained in this report. These restrictions information extracted from this document and used in derivative publications or briefings.



Reality Winner, Former N.S.A. Translator, Gets More Than 5 Years in Leak of Russian Hacking Report

ence ever imposed in federal court for an rmation to the media, prosecutors said.
ssociated Press

Force linguist and intelligence



TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

[redacted] DIRNSA

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any for

SUMMARY (U)

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian Genera
[redacted] executed
U.S. Company in August 2016, evidently to obtain inform
solutions, according to information that became availabl
from that operation to create a new email account and la
campaign targeting U.S. local government organizations
Word document trojanized with a Visual Basic script whi

Page 1

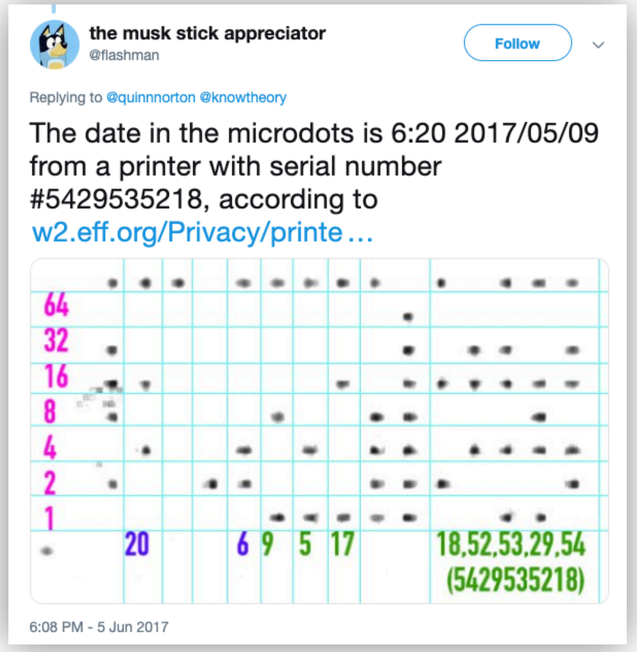
TOP SECRET//SI//ORCON

auf d
Testc

auf d
Testc

The Intercept had contacted the NSA on May 30 and sent copies of the documents in order to confirm their veracity.

The NSA notified the FBI of the situation and an official report from the FBI noted the documents "appeared to be folded and/or creased, suggesting they had been printed and hand-carried out of a secured space." Next, the NSA did an internal audit, confirming that Winner was one of six workers who had accessed the particular documents on its classified system, but only Winner's computer had been in contact with *The Intercept* using a personal email account.



The Intercept Should Have Known That The Document Contained Metadata And Retyped It To Be Safe

Information security types on Twitter have chastised the Intercept for not knowing that the printed document likely contained microdots or other metadata.

SwiftOnSecurity
@SwiftOnSecurity

Commentary: The microdot tracking thing is well-known in computer circles, if you were not aware of it before today. It's not secret. 1/4

♡ 142 6:51 PM - Jun 5, 2017

50 people are talking about this

SwiftOnSecurity
@SwiftOnSecurity

Replying to @SwiftOnSecurity

It's literally physical metadata. Which, like all documents with metadata, is hazardous to share raw with a motivated opposing party. 2/4

♡ 61 6:52 PM - Jun 5, 2017

16 people are talking about this

thaddeus e. grugq
@thegrugq

How did the intercept not know they're supposed to retype documents that are leaked to them to strip potential embedded metadata? twitter.com/ErrataRob/stat…

Rob Graham, will be at DEFCON/BSidesLV, hit me up @ErrataRob
Replying to @ErrataRob

So I wrote up a blogpost explaining how secret dots printers put on documents outed NSA leaker Reality

Hackers in China Attacked The Times

By NICOLE PERLROTH JAN. 30, 2013

Email

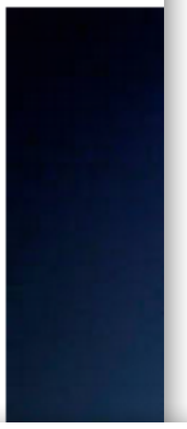
Share

Tweet

Save

More

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.



After surreptitiously tracking the intruders to study their movements and help erect

JAMES

Security experts found evidence that the hackers stole the corporate passwords for every Times employee and used those to gain access to the personal computers of 53 employees, most of them outside The Times's newsroom. Experts found no evidence that the intruders used the passwords to seek information that was not related to the reporting on the Wen family.

Even if you are not working on a sensitive story, **you are a target** if your colleagues are working on a sensitive story.

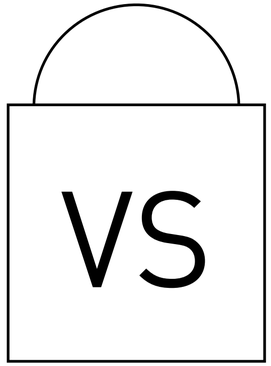
WHAT CAN YOU DO?

*Yes, you **CAN** do something!*

Passwords


OH SHOOT!
Someone figured out my PASSWORD...
now I have to rename my dog.
iapp.org

P4$$W0$RD#



SimplePassPhrase

Which do you think is stronger?

Password length is better than complexity

intel Security

Why?

Most websites you visit store your password in an encrypted format called a hash.

```
my_password = "0xF93A011443B3E2C31"
```

So, whenever you type your password into the system, it compares the hash of what you just typed, to the hashes stored in their database.

Password Dictionaries

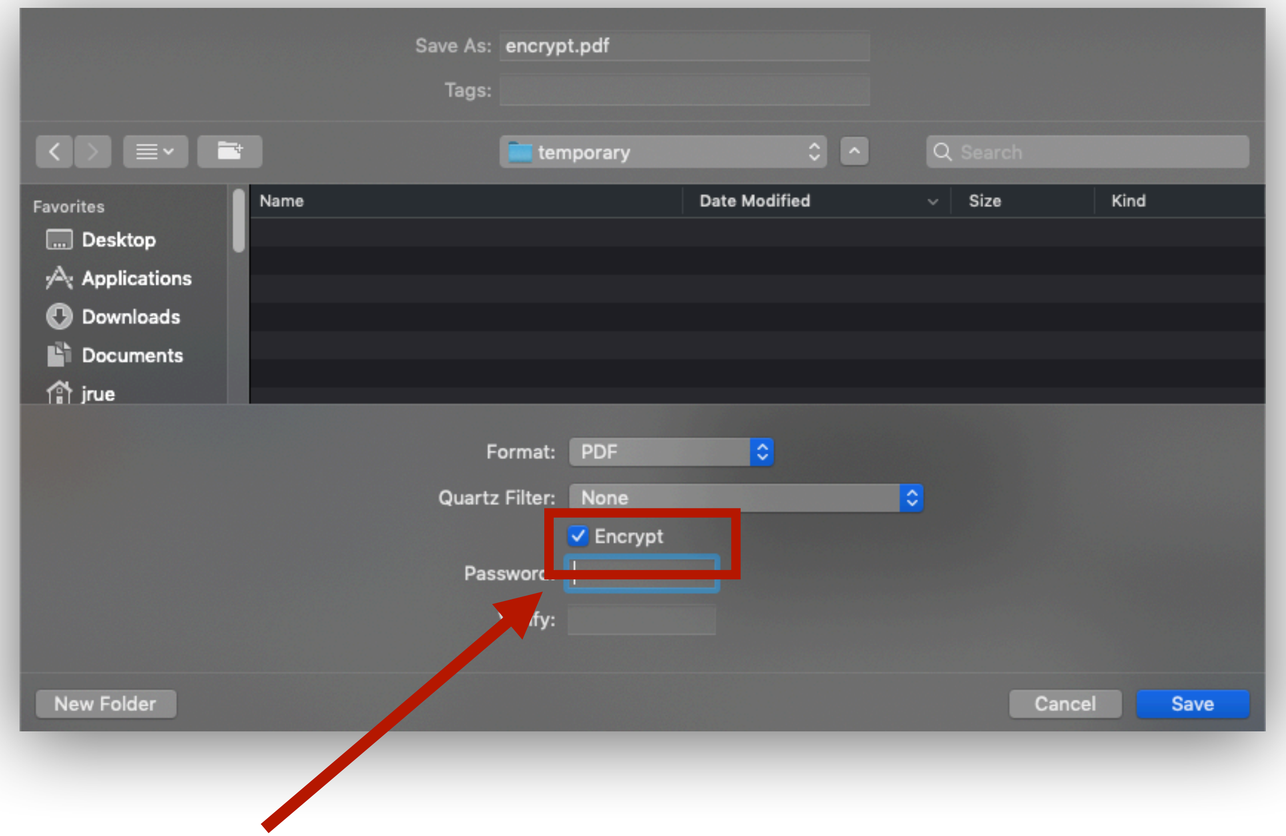
Password	Hash
123456	e10adc3949ba59abbe56e057f20f883e
password	5f4dcc3b5aa765d61d8327deb882cf99
12345	827ccb0eea8a706c4c34a16891f84e7b
12345678	25d55ad283aa400af464c76d713c07ad
football	37b4e2d82900d5e94b8da524fbeb33c0
qwerty	d8578edf8458ce06fbc5bb76a58c5ca4
1234567890	e807f1fcf82d132f9bb018ca6738a19f
1234567	fcea920f7412b5da7be0cf42b8c93759
princess	8afa847f50a716e64932d995c8e7435a
1234	81dc9bdb52d04dc20036dbd8313ed055
login	d56b699830e77ba53855679cb1d252da
welcome	40be4e59b9a2a2b5dffb918c0e86b3d7
solo	5653c6b1f51852a6351ec69c8452abc6
abc123	e99a18c428cb38d5f260853678922e03
admin	21232f297a57a5a743894a0e4a801fc3

Top 15 most common passwords in use.

"I just hacked a billion passwords by guessing 1-2-3-4-5."


LAST
WEEK
TONIGHT
WITH JOHN OLIVER

How long does it take to crack an encrypted PDF?



These sites have been hacked before

https://haveibeenpwned.com/

Solution?

Use a *unique* password for every service you use.

Password Managers

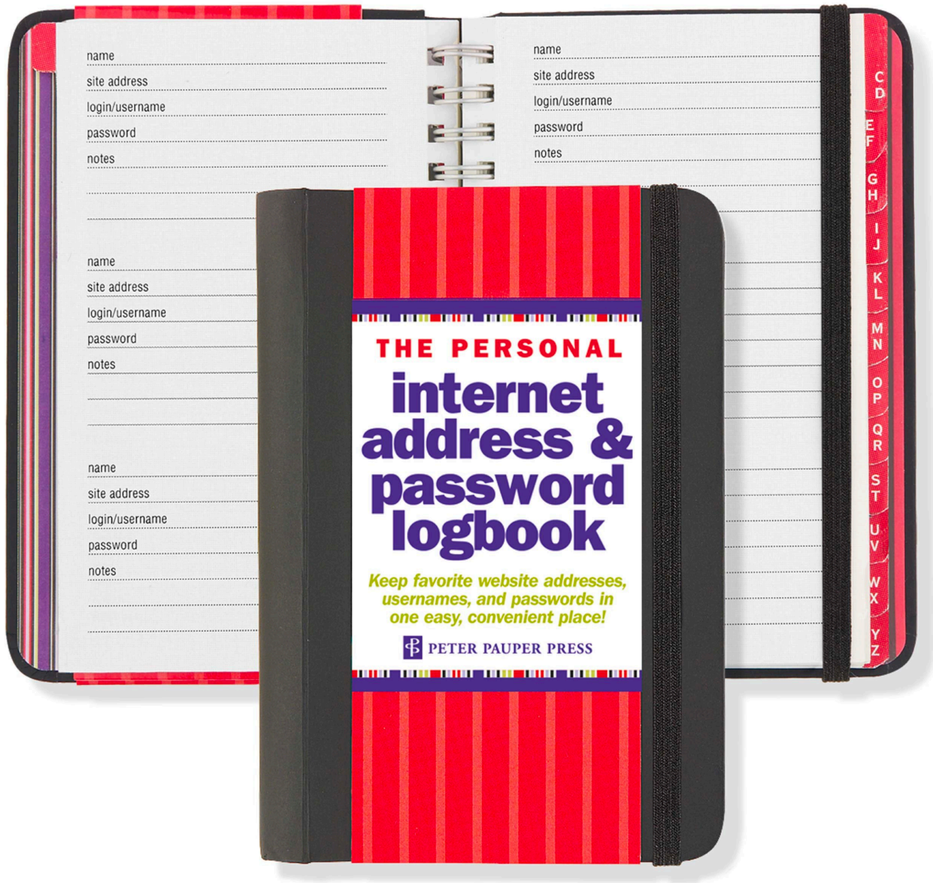
1password

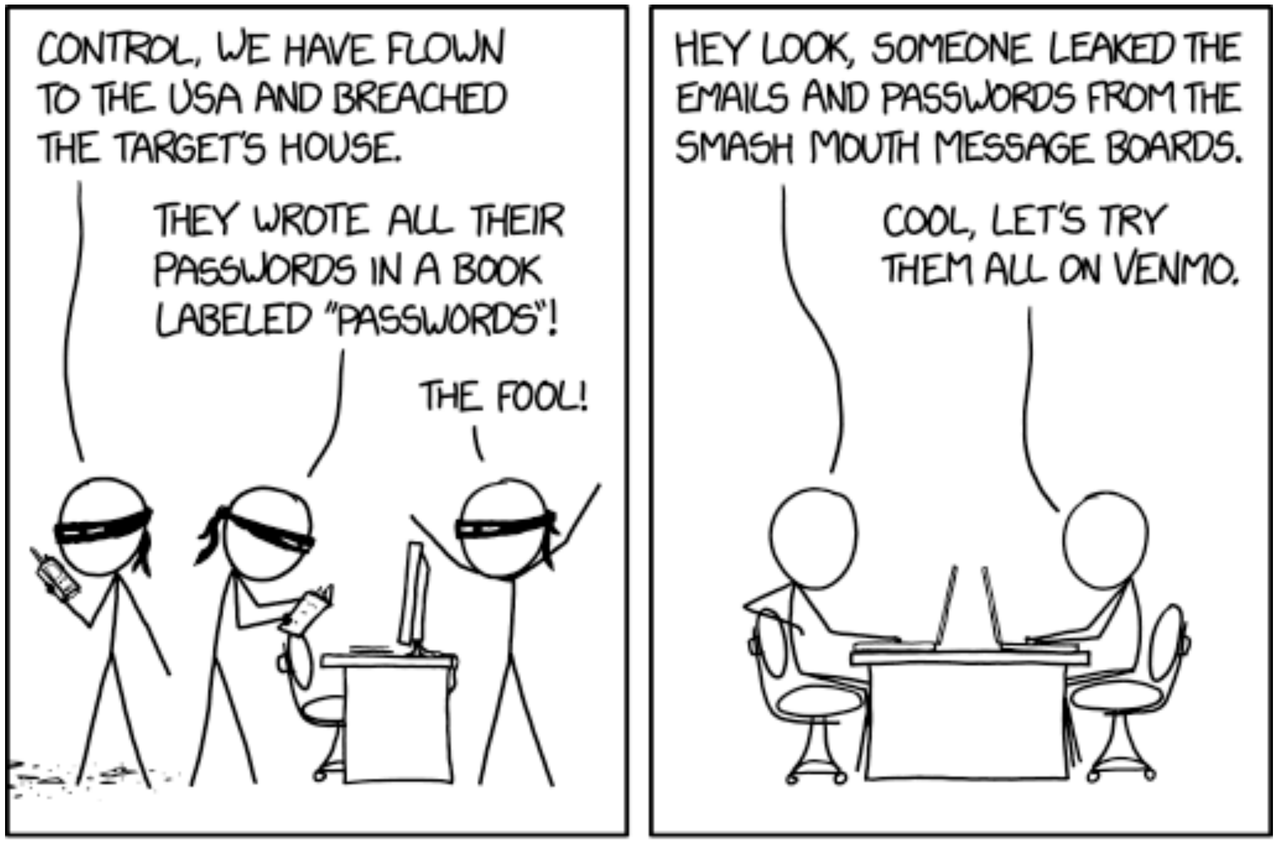
dashlane

LastPass ****

The Last Password You'll Ever Need.

KeePassX




CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.
THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!
THE FOOL!
HOW PEOPLE THINK HACKING WORKS
HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.
COOL, LET'S TRY THEM ALL ON VENMO.
HOW IT ACTUALLY WORKS

Access to one, means access to all

WIRED How Apple and Amazon Security Flaws Led to My Epic Hacking

DESIGN GEAR SCIENCE

MAT HONAN GEAR 08.06.12 8:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING

IN THE SPACE of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.

In many ways, this was all my fault. My accounts were daisy-chained together. Getting into Amazon let my hackers get into my Apple ID account, which helped them get into Gmail, which gave them access to Twitter. Had I used two-factor authentication for my Google account, it's possible that none of this would have happened, because their ultimate goal was always to take over my Twitter account and wreak havoc. Lulz.

How it happened

- Hackers went to his personal website, and found his gmail address.
- Then they did account recovery, and it shows alternate email obscured as m••••n@me.com (they didn't actually attempt recovery).
- me.com is run by Apple. They just needed billing address. They looked to see how he bought his web domain, and got his home address.
- They called Amazon and told them they were the account holder, and wanted to add a credit card number to the account. All you need is the name on the account, an associated e-mail address, and the billing address. Amazon then allows you to input a new credit card.
- Then they hung up. Next they called back, and told Amazon they lost access to the account. Upon providing a name, billing address, and the new credit card number they gave the company on the prior call, Amazon allowed them to add a new e-mail address to the account.
- Once in Amazon, they could see all the credit cards on file for the account – not the complete numbers, just the last four digits. But, Apple only needs those last four digits to reset an email.

Other solution: 2-Factor Authentication

Phishing

Sent: Tue 4/23/2013 12:12 PM
From: [An AP staffer]
Subject: News

Hey,

Did you see this?

http://www.washingtlonpost.com/blogs/worldviews/wp/2013/04/23

[From a different AP staffer]
Associated Press
San Diego
mobile

Sent: Tue 4/23/2013 12:12 PM
From: [An AP staffer]
Subject: News

Hey,

Did you see this?

http://www washingtlonpost com/blogs/worldviews/wp/2013/04/23

[From a different AP staffer]
Associated Press
San Diego
mobile

www.washingtlonpost.com

Dear User,

This message is to inform you that your access to bCourses will soon expire. You will have to login to your account to continue to have access to this service.

You need to reactivate it just by logging in through the following URL. A successful login will activate your account and you will be redirected to your bCourses page.

http://bcourses.berkeley.cnea.gq/login_0DZbL4B22o0ki22F0lZotK2LqgZijDXvflrGID3D4cemh3lPfYHa62pNgFo4Oh4B40F

If you are not able to login, please contact Mary Patel at mpatel@berkeley.edu for immediate assistance.

Sincerely,

Mary Patel
Berkeley Security
University of California, Berkeley
510-643-6927
mpatel@berkeley.edu

Campus examples of Phishing:

https://security.berkeley.edu/resources/phishing

This is the website you're on.

[subdomain].[subdomain].[**DOMAIN**].[TLD]

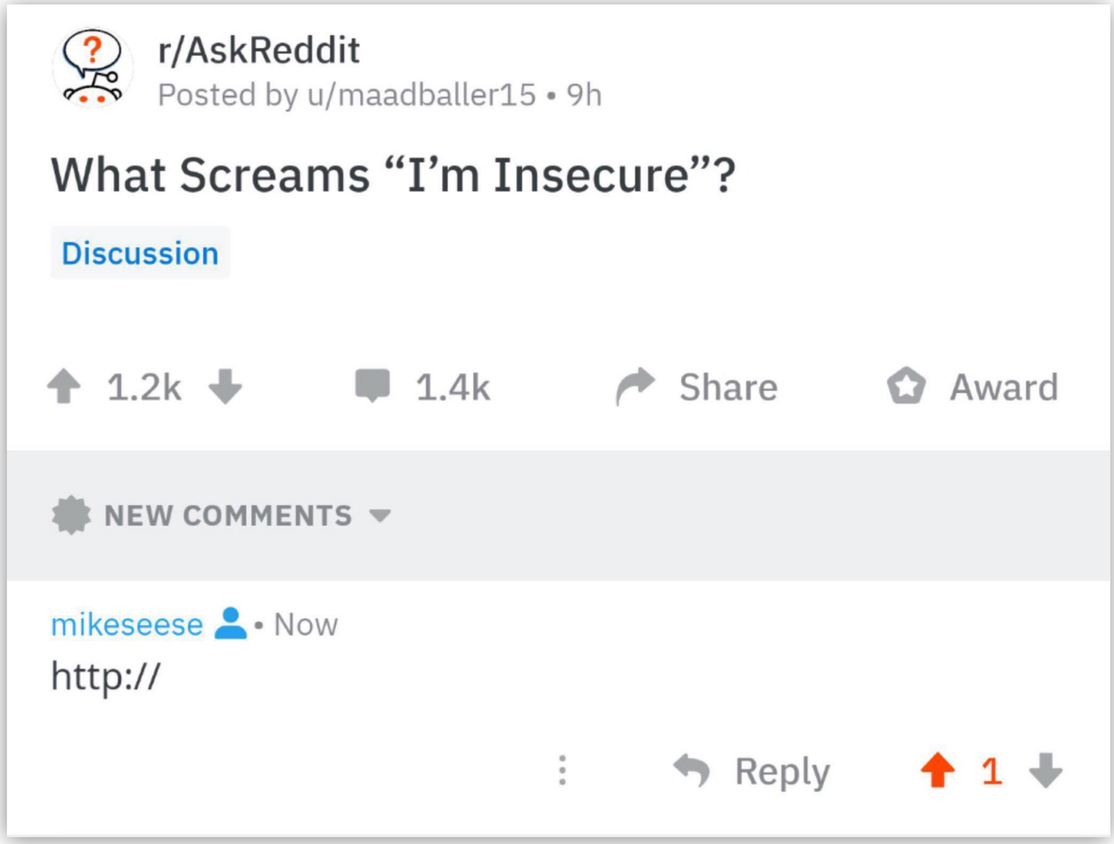
Example: https://multimedia.journalism.berkeley.edu

[*anything*].[*anything*].[DOMAIN].[TLD]

bcourses.berkeley.cnea.gq ← Fake website

bcourses.berkeley.edu ← Real website

Make sure the website is https



Spearphishing

The spear phisher thrives on familiarity. They know your name, your email address, and at least a little about you.

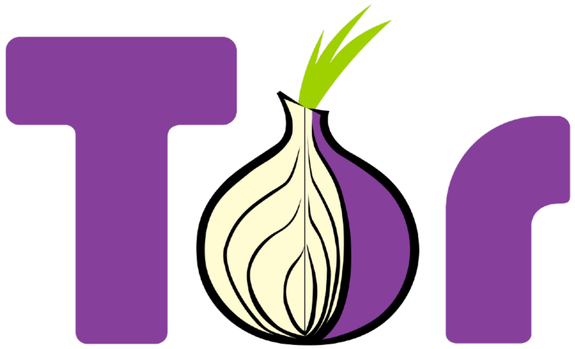
But all is not lost, if you're alert

Preventing Spearphishing

- The most common attack against journalists specifically, relies on getting the user to visit a site under false premises.
- Typically, it directs users to a fake login page to trick them into entering passwords.
- **SOMETIMES**, all you have to do is just visit a malicious page. (Generally, this relies on using a special hack that exploits a weakness in the browser or operating system, and is usually avoidable by keeping your computer updated.)
- Read the URL before clicking a link from a message. ALWAYS read the URL before entering a password.

Advanced Threats

Tools are not magic



Know when to use them, and what they're good for, and what limitations they have.

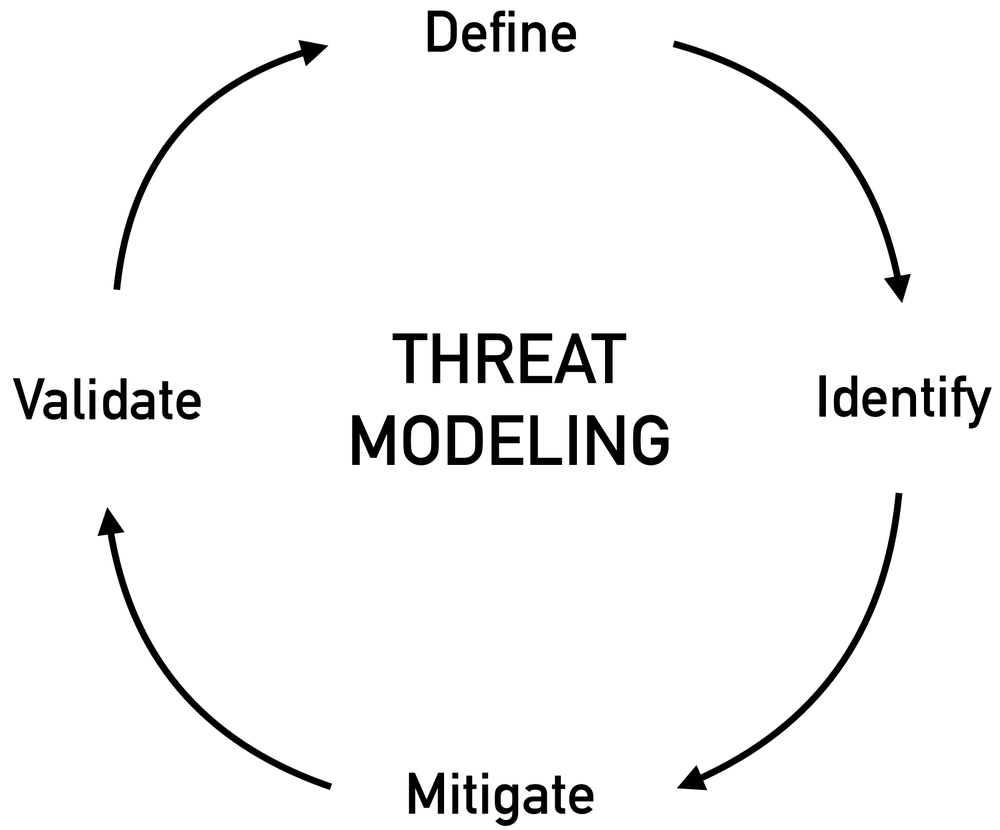
Threat Modeling

- **Define what you're trying to protect**.
  What are you trying to prevent happening? Getting hacked? Identifying a source? Protecting your privacy?

- **Identify your adversaries.**
  Who are your adversaries? What are their capabilities? Is it a stalker? An ex-boyfriend? The fbi or nsa? A foreign government?

- **Mitigate your threats.**
  Take steps to compartment your information to lessen the damage in worst case scenario.

- **Validate your decisions.**
  Study real-world examples, and learn from experience.



Scenario: You meet a friend who works at a bank

- You’re at a coffee shop during lunch and your friend says, "There is some serious unethical stuff going on at our bank. It’s really sleazy. They are preying on elderly communities, signing them up with super high-interest loans. The bank persuades them, when really it isn’t in their best interest. It’s not illegal per se. But it’s bad enough to make anyone’s stomach turn."

- The friend has a load of documents **on her work computer** proving these practices, including a video footage of seminars given in elderly communities.

- She wants to help you (a journalist) to get the word out.
  Threat model this scenario.

Threat Model: Bank Scenario

- **Define:** What are the potential threats both you and the source could face in this situation?
- **Identify:** Who are the adversaries? What are their capabilities?
- **Mitigate:** What steps could you take to protect your source, the information, and yourself in this scenario?
- **Validate:** Look at similar past situations. Maybe talk to IT people about the technical capabilities of a bank.

Would Email Encryption Work? Why or why not?

Hey there, how are you doing?

```
-----BEGIN PGP MESSAGE-----

hQEMA3DdQN0NsOyFAQf9HdJJNbQc4GFwnMf9OzGUrTetNZ8sJCo3EEKhDBE7dSTZ
OO2UO8UMz6KKRVdWuGY/6dkoIxsadiPJ4Ub5fkO5MHSDY+xaOrqqBFehvh0wfCTM
hqn0mWyiF8P3Mm6IZeoM7c9bCTFzzWvxIqR9H4gJM4YbW4WFrIawKxFlFc+jjwLf
jvdL96e5u4kN9CxztBRkRGe81Ns0l+GK0gvP+XMOb3j/MiA3fJMCjsr/a84MoF1R
a8FxDkOpyWsQZ9asK+PmnyCTsECj5iHO5A6kL3/ULfg3V627r8LwSPdeaV41bhn6
5c/vz/ppXZozZkkiDS+xTq5GYUBPjGwrKqUu47mwwNJgAe77C5upAzX4/8bHmrlI
uaUCq3EUM4K95oithFkUWg0Al6J5lx5FWuHPvgg566Kj41kfLDOyUoqhszSMmeST
FiN6v7jnxWU+i9Jtp908uQFC0Ae8tBCxlS9uwYMIui5p
=thuz
-----END PGP MESSAGE-----
```

Scenario: Egyptian Activists

- You're a photographer in Egypt covering demonstrations against police brutality. You have photographs of many of the protestors and activists that are resisting the government and police force. You capture photographs of individuals, their faces, and in some cases, in their homes, while photographing. You probably won't publish these, but you have them all on your camera's memory card.

- After several days, you've completed your assignment and it's time to head back home. You know that you'll have to get though customs at the airport, and risk facing a security screening.

- Threat model this situation.

Threat Model: Egypt Scenario

- **Define:** What are the potential threats both you and your sources face in this situation?
- **Identify:** Who are the adversaries? What are their capabilities?
- **Mitigate:** What steps could you take to protect your sources, the information, and yourself in this scenario?
- **Validate:** Look at similar past situations. What do security screenings generally require?

Compartmentalize

Separate and wall off areas of your life/work

- Always consider **what might happen if you fail**. How do you mitigate the damage?
- Some journalists use burner phones for different sources. Or different laptops for their work (or specific stories).
- Create separate social media accounts for different purposes.
- Create separate email accounts for different situations/stories.
- Using different credit cards for different types of purchases. Using different web browsers for different searches.
- What else?

Embrace non-digital tradecraft

- Old school meeting in-person is actually some of the best tradecraft techniques. Depending on your threat model, leave your cell phone at home. (What other risks exist with this?)

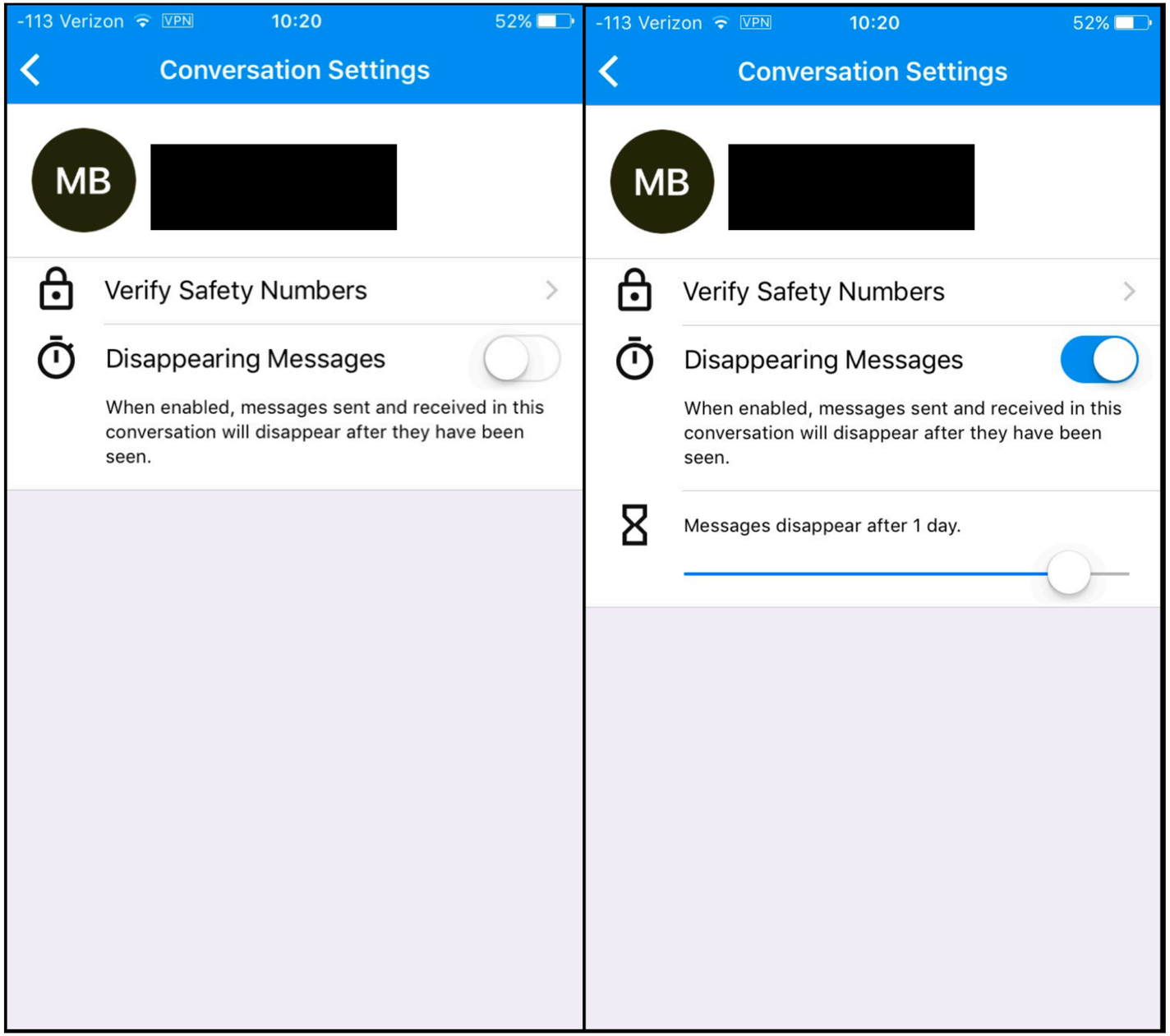
- U.S. Postal Mail works remarkably well. (Trump's tax returns sent to the NYTimes.)

- Other tradecraft techniques (change on laptop in hotel safe).

Tools

Encrypted communication: Signal

- Signal app is end-to-end encrypted. The signal company doesn't have access to the messages at any point in time, nor the keys to unlock the messages. They keys exist on each person's phone who is receiving the message.
- Non-profit, donation funded. Open source, and code audited by security researchers.
- Used by journalists, politicians, activists, etc. Currently endorsed by ACLU.
- **WhatsApp** also uses the same Signal protocol, but isn't audited and is owned by Facebook.



Turn on disappearing messages

Set how long it takes for messages to disappear.

Mueller says use of encrypted messaging stalled some lines of inquiry

Zack Whittaker @zackwhittaker

A single paragraph in the Mueller report out Thursday offers an interesting look into how the Special Counsel's investigation came head-to-head with associates of President Trump who used encrypted and ephemeral messaging to hide their activities.

From the report:

> Further, the Office learned that some of the individuals we interviewed or whose conduct we investigated-including some associated with the Trump Campaign — deleted relevant communications or communicated during the relevant period using applications that feature encryption or that do not provide for long-term retention of data or communications records. In such cases, the Office was not able to corroborate witness statements through comparison to contemporaneous communications or fully question witnesses about statements that appeared inconsistent with other known facts.

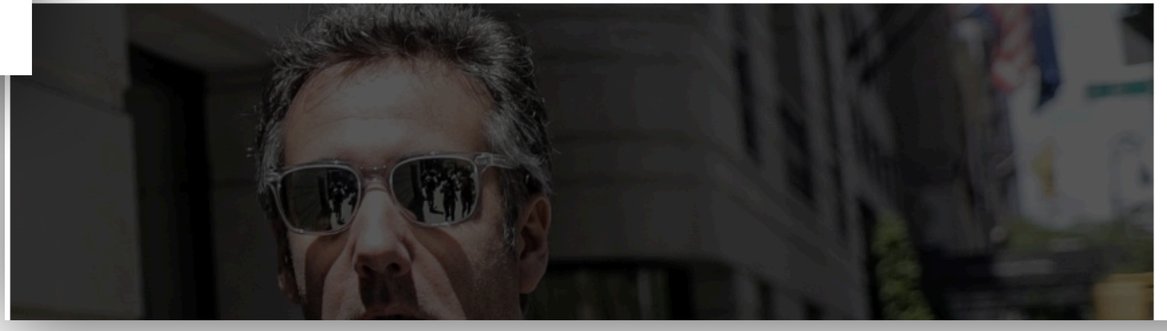
POLITICS JUNE 15, 2018 / 1:30 PM / A YEAR AGO

U.S. prosecutors pull encrypted messages from phones seized in Cohen raids

Brendan Pierson

3 MIN READ

NEW YORK (Reuters) - Federal prosecutors investigating U.S. President Donald Trump's longtime personal lawyer Michael Cohen have extracted more than 700 pages of messages sent using encrypted programs like WhatsApp and Signal on phones seized from Cohen, according to a court filing on Friday.

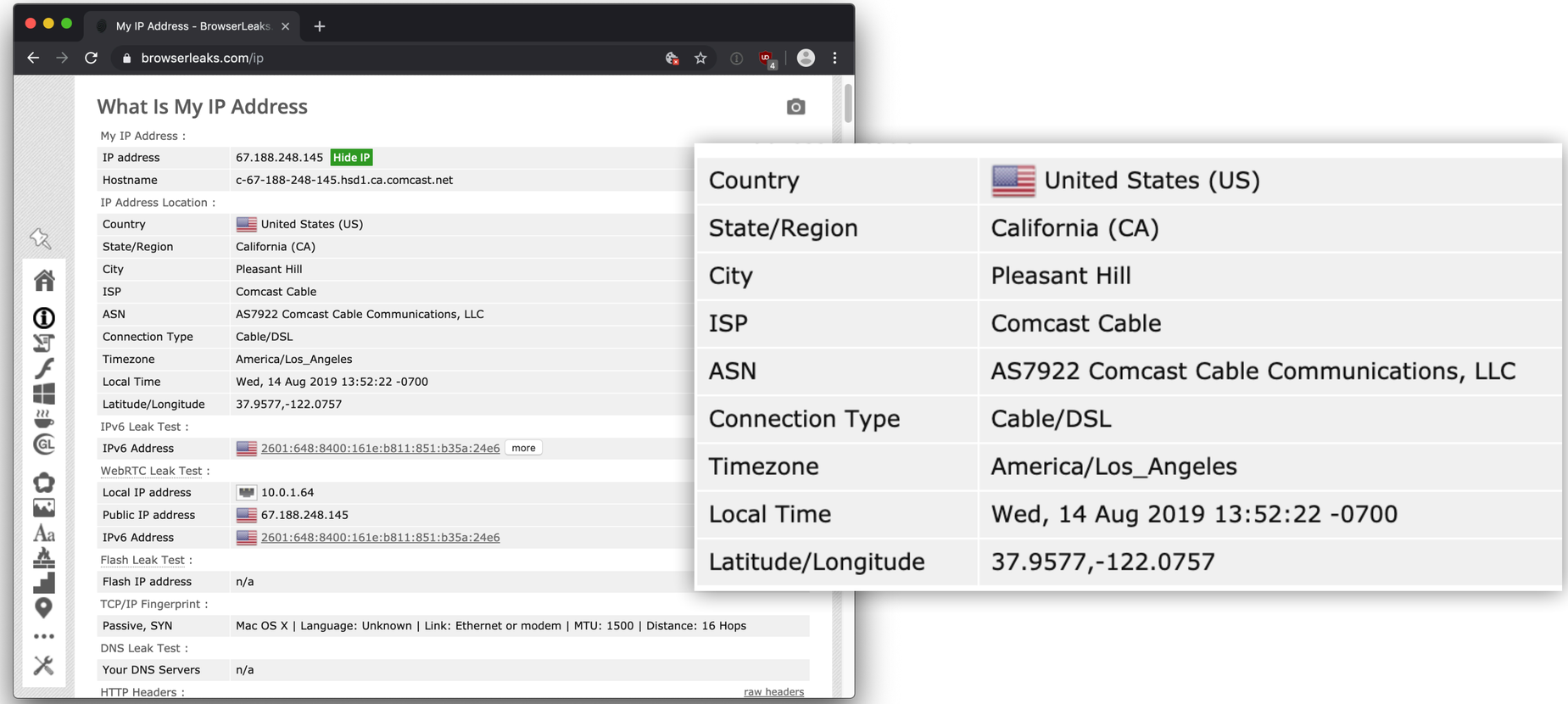


Virtual Private Network (VPN)

- **Privacy:** Used when you don't want the websites you visit to know who is visiting them.
- **Security:** It's also used in untrusted Wifi situations, like airports or cafes, to ensure no one is tapping your connection, since it's encrypted.
- **Circumvent location restrictions:** Lastly, it's used to appear as if you're using the internet from a different location. Sometimes this is to get around firewalls, or location restrictions (e.g. Visiting China, or to watch YouTube videos restricted to another country).

What Websites Know About You

https://browserleaks.com/ip



What websites know about you:

- **Your IP address**, and thus the general location from which you connect to the internet. e.g. UC Berkeley. Or, they know who you pay for internet (i.e. Comcast or AT&T.)

- **The website** you just came from, if you clicked a link.

- **The type of browser** you're using, the size of your screen. The motion of your trackpad/mouse, the orientation of your phone, sometimes the name of your computer.

- **Cookies and other tracking** data, can also reveal your entire search history. Basically, they have advertisements which fingerprint you. And when you visit other sites, they can see you're the same computer that went to several websites.

- http://bit.ly/propublica-fingerprint-article

See what Google Knows...

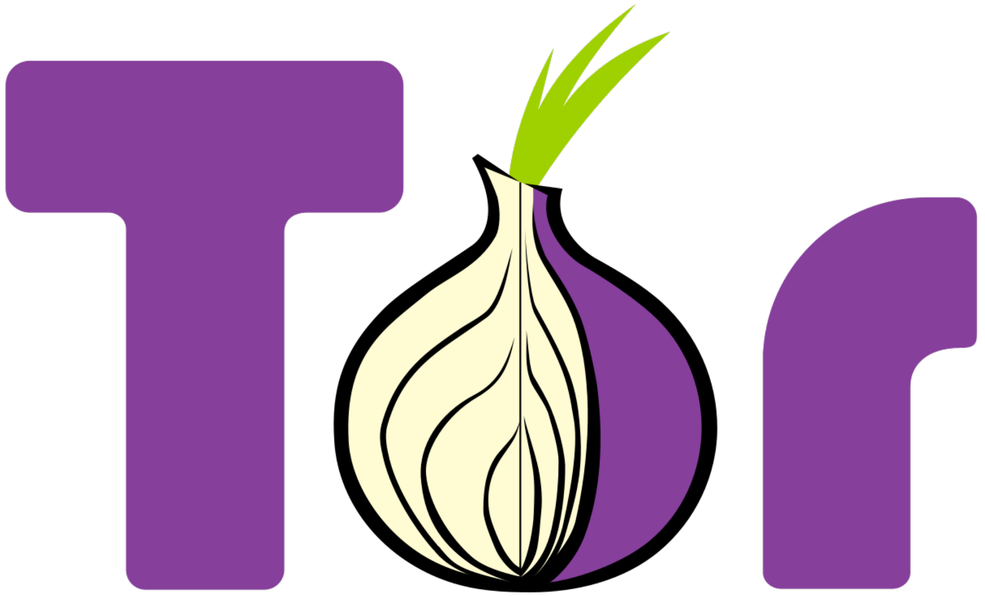
- See how Google categories your advertising preferences: **https://www.google.com/settings/ads/**
- See how Google tracks your location history: **https://maps.google.com/locationhistory**
- See how Google keeps track of your web search history: **https://www.google.com/history/**
- See what apps have access to your account: **https://security.google.com/settings/security/permissions**

Tor Browser

- **Anonymous.** Tor is a special anonymized network of computers worldwide. When you connect to this network, you're completely anonymous when you visit websites. They know nothing about you.

- **The Dark web.** There are certain websites that have the TLD .onion, that are only accessible via Tor. Sometimes called the dark web, these websites cannot only track visitors, the web servers themselves are a mystery.

- **Used by activists, privacy advocates, illegal uses?** Tor is famous for facilitating illegal dealings, such as the famed Silk Road drug market. It's also been widely associated with Torrents (illegal downloading of pirated movies and music) and certain types of illicit pornography.

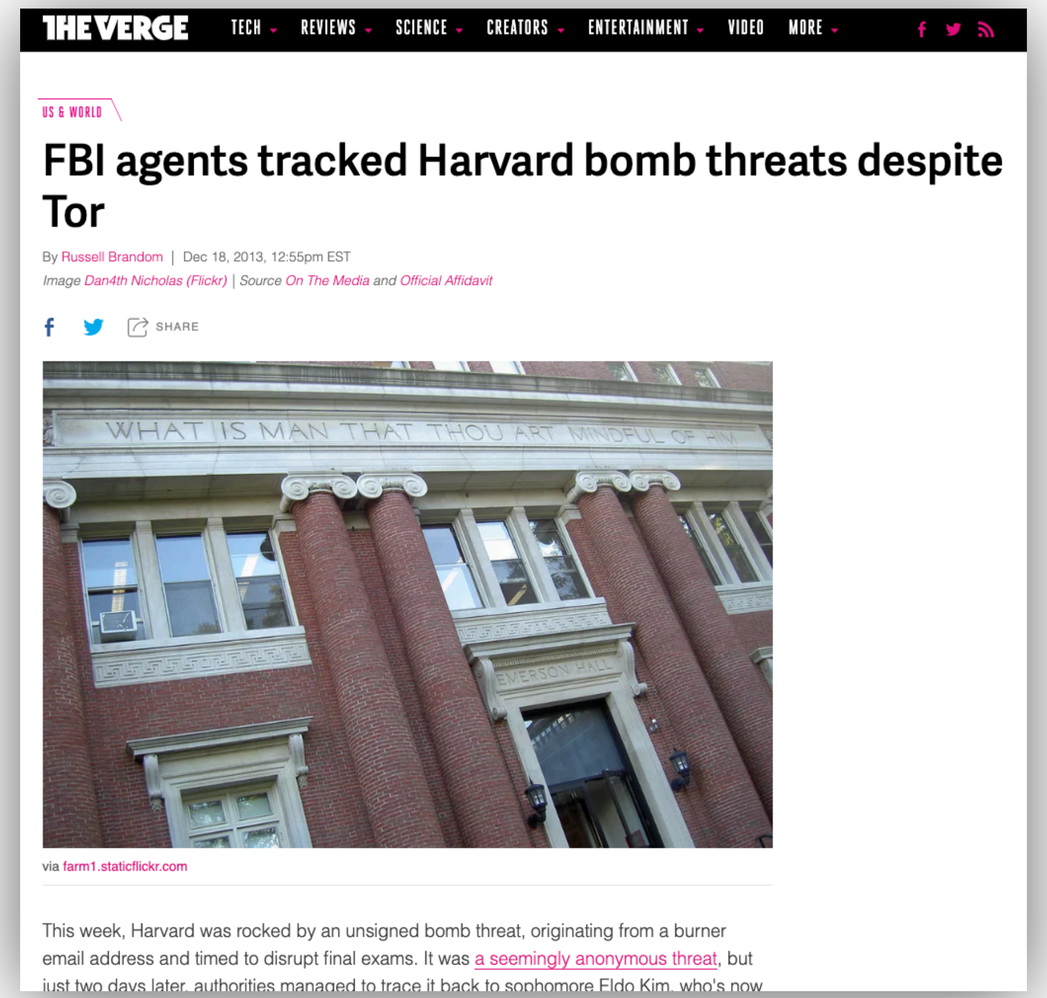


Case Study

- Your ISP (internet service provider) can see if you connect to the Tor network. They don't know what sites you visit, but they do know you're on the Tor network.

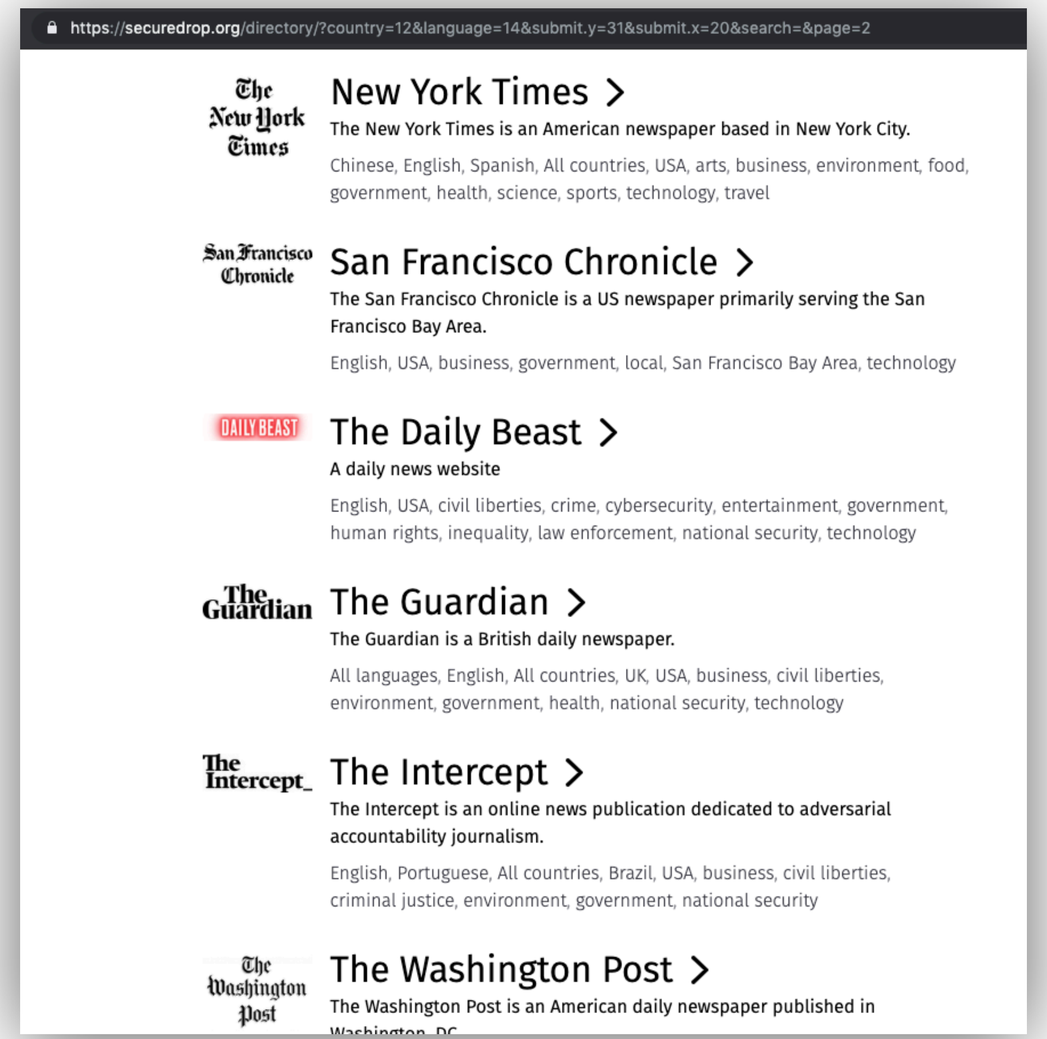
- Harvard student tried to get out of final exams by emailing a bomb threat to the school. They canceled class, and postponed the test.

- The email was sent anonymously, but the FBI could see that it was sent from an anonymous services via Tor. They checked the logs, and they saw that only one person on all of Harvard campus was connected to the Tor network at the time the email was sent. They caught student Eldo Kim. He served 4 month in home confinement, had to pay thousands in restitution, and issue an public apology.



Secure Drop

- Uses the Tor network to share news tips with news publications. They will give you instructions to download the Tor Browser.
- The tips are completely anonymous, and even state actors like NSA or FBI wouldn't be able to tell where those messages came from.
- Most news organization corroborate information before running any stories. So you're unlikely to fool them with fake information.



PGP/GPG Pretty Good Privacy

- **Text/File Encryption program** that is often used to send encrypted messages. You can also encrypt files.
- **Both parties must have GPG installed**, and have previously setup and shared "keys" for sending messages.
- You can actually post a **public version** of your PGP key online, so anyone can send you encrypted messages that only you can unlock.
- Requires some technical knowledge. While considered impenetrable, it has lots of issues. **The key is a single point of failure.**

keybase.io

- A website where people post their PGP keys. You can find lots of journalists, activists, politicians, and others there.
- You can encrypt messages and email the cypher to them.
- You can verify the key belongs to the right person through various verification methods.

Key Exchange Party

Key party

From Wikipedia, the free encyclopedia

Key party may refer to:

- A key party, a type of group sex event
- A key signing party, an event at which people present cryptographic keys to others in person for identity verification

*This disambiguation page lists articles associated with the title **Key party**.*

If an internal link led you here, you may wish to change the link to point directly to the intended article.

Crypto Key Exchange Party

Key signing party

From Wikipedia, the free encyclopedia

In public-key cryptography, a **key signing party** is an event at which people present their public keys to others in person, who, if they are confident the key actually belongs to the person who claims it, digitally sign the certificate containing that public key and the person's name, etc. Key signing parties are common within the PGP and GNU Privacy Guard community, as the PGP public key infrastructure does not depend on a central key certifying authority, but to a distributed web of trust approach. Key signing parties are a way to strengthen the web of trust. Participants at a key signing party are expected to present adequate identity documents.

Although PGP keys are generally used with personal computers for Internet-related applications, key signing parties themselves generally do not involve computers, since that would give adversaries increased opportunities for subterfuge. Rather, participants write down a string of letters and numbers, called a *public key fingerprint*, which represents their key. The fingerprint is created by a cryptographic hash function, which condenses the public key down to a string which is shorter and more manageable. Participants exchange these fingerprints as they verify each other's identification. Then, after the party, they obtain the public keys corresponding to the fingerprints they received and digitally sign them.

Key signing in front of FOSDEM 2008.

See also [edit]

- Zimmermann–Sassaman key-signing protocol
- Web of trust
- CryptoParty

VeraCrypt

- Allows you to create an encrypted external hard drive or thumb drive.
- **Allows for hidden volumes** (you stick in a thumb drive and see nothing, and it appears like it's empty. Only if you have VeryCrypt installed and know the password before hand, can you see if data is really there.)
- **Plausible deniability.** You can create two drives with separate passwords. So you give your adversary the decoy password, and they see files you planted intentionally.
- **Works best on PC.** Mac technically work with additional software installed.

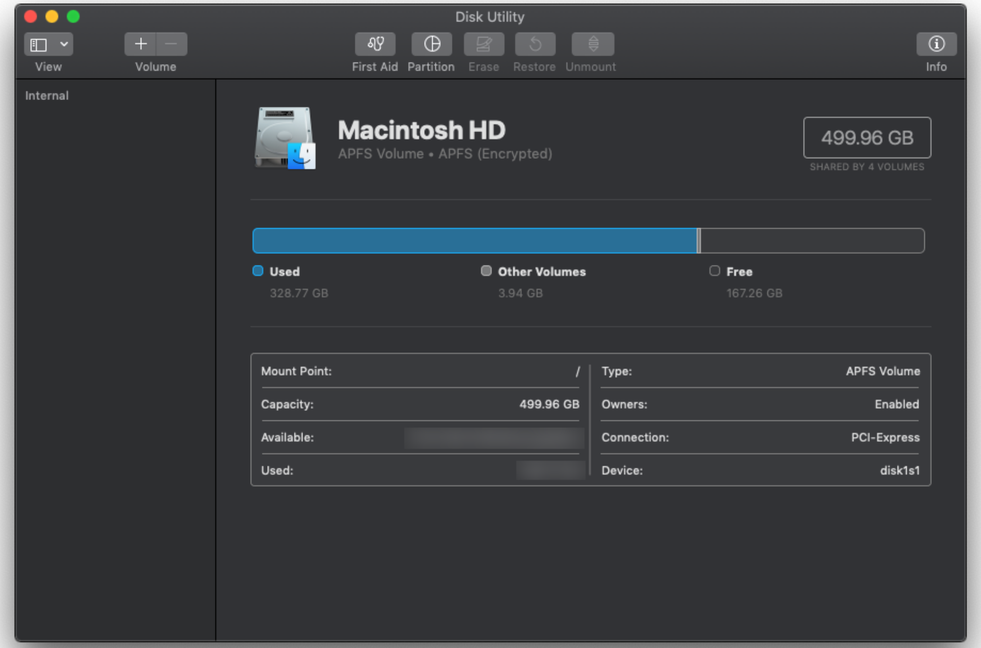
Mac DiskUtility

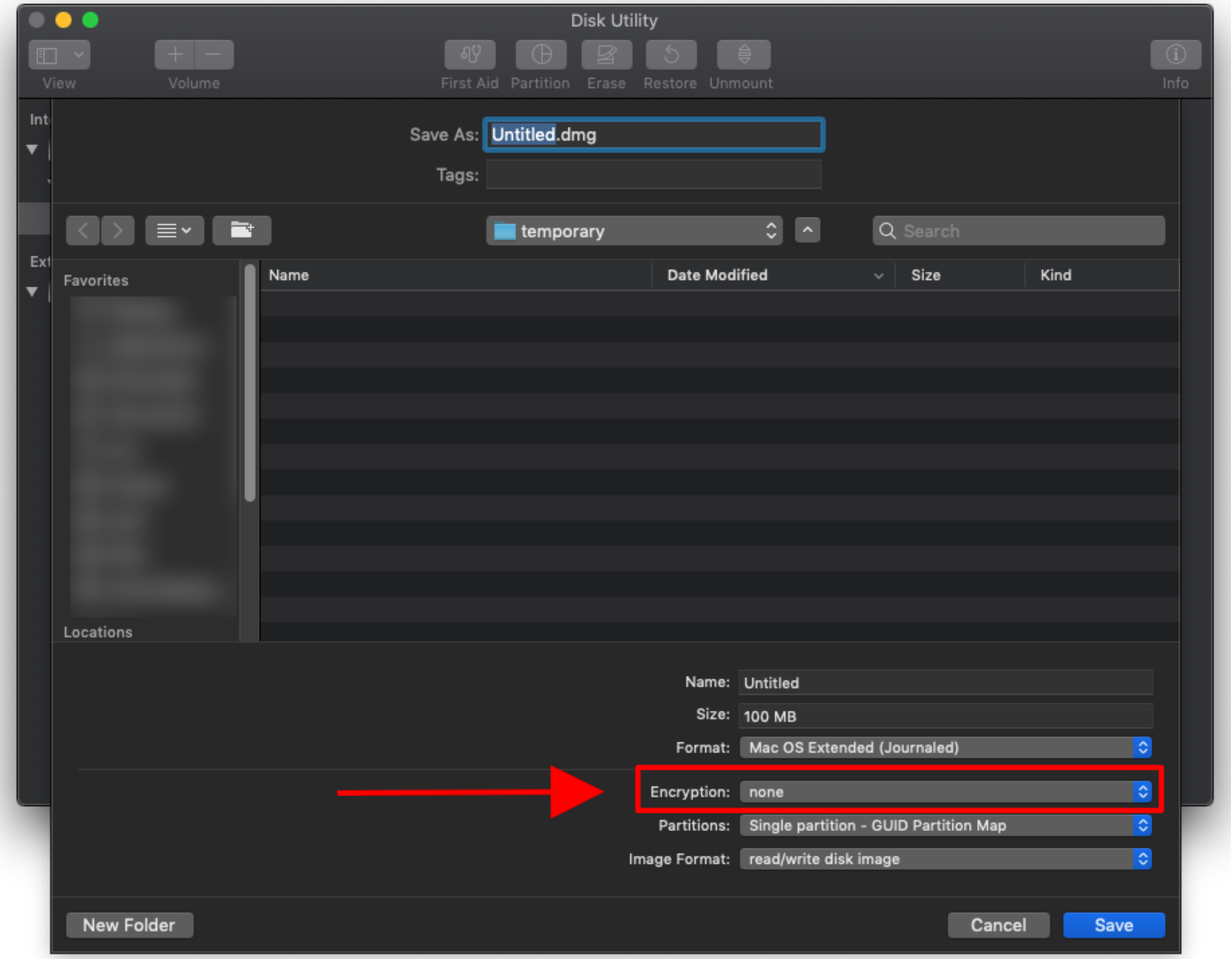
- **Allows you to create encrypted folders** on your Mac. But without the hidden volume or plausible deniability of VeraCrypt.

- **Open DiskUtility** software on your Mac (you can search for it.) It's in the Utilities folder in Applications.

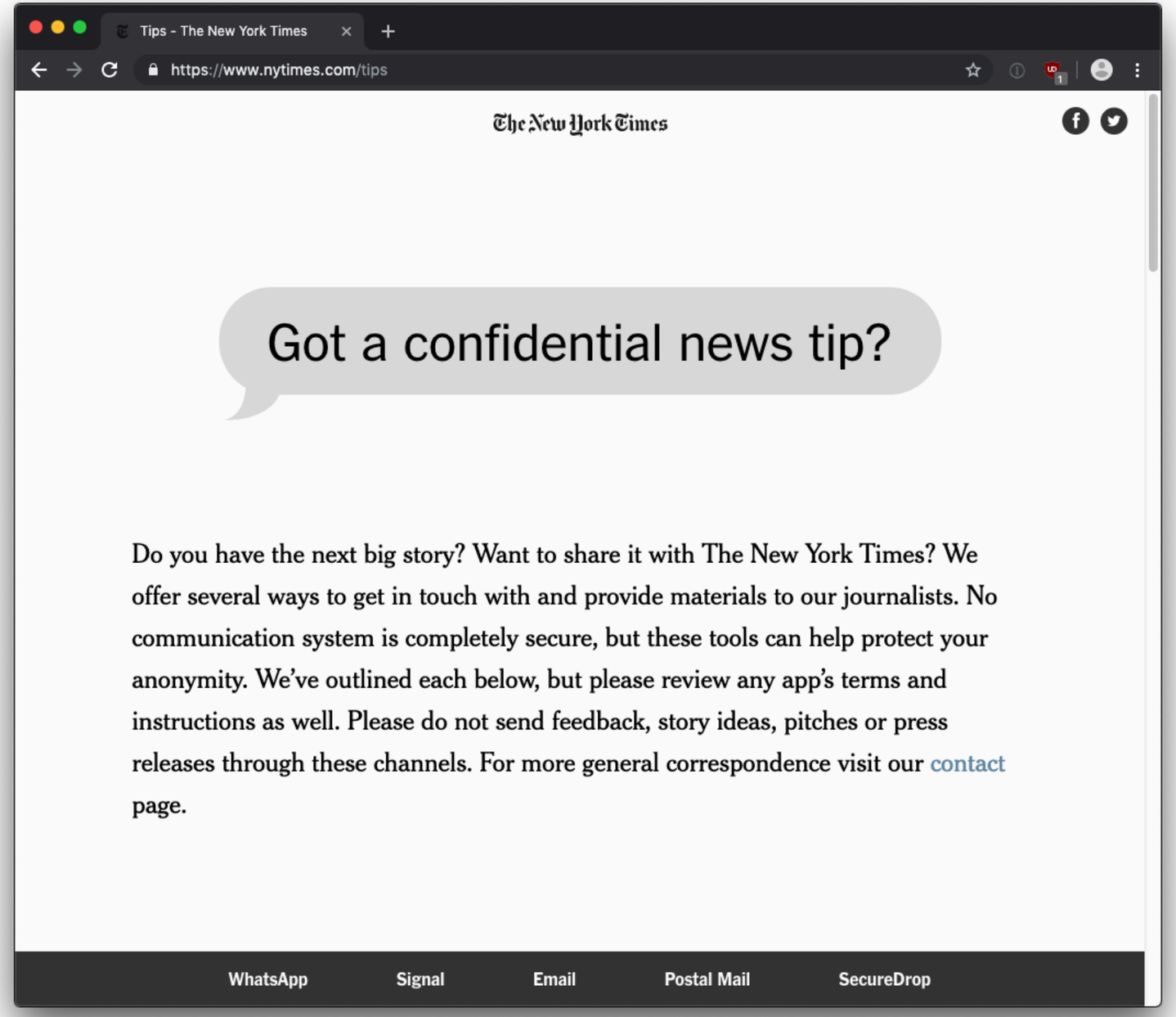
- **The folders can be transferred to external drives**, but won't work on PCs or other computers. It's Mac only system.

Disk Utility





1. Open DiskUtility
2. Click File —> New Image (Blank Image)
3. Set your Encryption
4. Set a size for the folder (called Volume).
   You can resize it later if needed.


Tips - The New York Times
https://www.nytimes.com/tips
The New York Times
Got a confidential news tip?
Do you have the next big story? Want to share it with The New York Times? We offer several ways to get in touch with and provide materials to our journalists. No communication system is completely secure, but these tools can help protect your anonymity. We've outlined each below, but please review any app's terms and instructions as well. Please do not send feedback, story ideas, pitches or press releases through these channels. For more general correspondence visit our contact page.
WhatsApp
Signal
Email
Postal Mail
SecureDrop